

UNITED STATES DISTRICT COURT

for the
Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH DROPBOX USER
shawn.marlow2020@gmail.com THAT IS STORED AT
PREMISES CONTROLLED BY DROPBOX, INC.

Case No. M-25 -414-CMS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached and incorporated by reference.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A(a)(5)(B)	Possession of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Marisol Flores, FBI.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Marisol Flores, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: July 3, 2025

City and state: Oklahoma City, Oklahoma



Judge's signature

CHRIS M. STEPHENS, U.S. MAGISTRATE JUDGE

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Marisol Flores, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Dropbox, Inc. ("Dropbox"), an electronic service provider headquartered at 1800 Owens St., Ste. 200 San Francisco, CA 94158. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the account, including the contents of communications.

2. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) since May 2015, and I am currently assigned to the Oklahoma City Division. Since joining the FBI, I have been involved in investigations of child exploitation matters and computer crimes against children. I am currently assigned to investigate violations of federal law involving the exploitation of children. I have gained expertise in conducting such investigations through in-person trainings, classes, and everyday work in my current role as an SA with the FBI. Moreover, I have access to the institutional knowledge developed around this type of investigation by working with other experienced child exploitation criminal investigators. I have become aware of numerous examples of

child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, to include electronic media.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(5)(B), Possession of Child Pornography, have been committed by Shawn MARLOW using the Dropbox account associated with **shawn.marlow2020@gmail.com**. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On March 14, 2025, at 20:41:22 UTC, Media Lab/Kik Electronic Service Provider submitted a CyberTip to the National Center for Missing and Exploited Children (NCMEC) regarding Kik Username: smh2022_c3t communicating with another Kik user

how smh2022_c3t sexually abused their younger sister. Media Lab/Kik provided the following information to NCMEC:

Name: Shawn Me

Address: Fort Smith, AR US

Date of Birth: [XX]-[XX]-1992

Email Address: **shawn.marlow2020@gmail.com**

All email addresses reported? Yes

ESP Product/Service: Kik

Screen/User Name: smh2022_c3t

Display Name: smh2022

ESP User ID: smh2022_c3t

Compromised Account? No

IP Address: 12.75.0.97 03-13-2025 17:30:00 UTC

Estimated Location: Fort Smith, Arkansas, US at 03-13-2025 17:30:00 UTC

7. Media Lab/Kik described in their information to NCMEC the above user communicated the following to another user in a private chat on January 13, 2025, 02:23:27.014000 UTC:

“I started eating my sisters pussy when she was 6 and I was 13 she sucked my dick and swallowed my cum first time and 6 months later”

8. On March 28, 2025, at 09:10:32 UTC, Media Lab/Kik Electronic Service Provider submitted a CyberTip to the NCMEC regarding Kik Username: smh2022 distributing pornography to another Kik user in a private chat. Media Lab/Kik provided the

following information to NCMEC:

Kik Messenger

Email Address: **shawn.marlow2020@gmail.com**

ESP Product/Service: Kik

Screen/User Name: smh2022

Display Name: Shawn Me

ESP User ID: smh2022_c3t

Media Lab/Kik described in their information to NCMEC the above user uploaded a video and an image to another user in a private chat. Those files are described in the following paragraphs.

9. The video file, 2c9d6ba1-58ef-4c88-93e3-1dc50690367c.mp4, was uploaded on March 20, 2025, at 13:26:14 UTC. This video was one minute and forty seconds in length. The video depicted a prepubescent female, whose face was visible from the camera view, with a pink, short sleeve shirt on. The prepubescent female was performing oral sex on a pubescent female of an indeterminate age, who was naked from at least the waist down. The prepubescent female continues to perform oral sex on the other female while the other female is both standing and sitting throughout the video.

10. The image file, 4eb0c4de-cb4a-432c-95a5-60bcf03e383a.jpg, was uploaded on March 20, 2025, at 13:24:44 UTC. This image depicted a prepubescent female lying on her back, naked from her chest down exposing her breast area and vagina. Standing next to the child is an adult male visible from the waist down with an erect penis. The prepubescent female is holding the adult male's erect penis with both of her hands.

11. On March 26, 2025, an administrative subpoena was served to Kik, through its parent company MediaLab.ai. On May 3, 2025, Kik, through its parent company MediaLab.ai, provided information regarding email address: **shawn.marlow2020@gmail.com**; screen/user name: smh2022_c3t; display name: smh2022; ESP User ID: smh2022_c3t pursuant to an administrative subpoena served on March 26, 2025. The following is a portion of the information provided by Kik:

Date: May 3, 2025

First Name: Shawn

Last Name: Me

Email: **shawn.marlow2020@gmail.com**

Username: smh2022

Login IP: 70.182.93.83 52886 2024-10-13 16:58:45 CAN

Login IP: 70.182.71.46 59740 2024-11-10 18:00:02 CAN

Login IP: 70.182.71.46 53556 2025-02-16 18:01:00 CAN

12. On March 26, 2025, an administrative subpoena was served to Google Inc. to provide information pertaining to email address: **shawn.marlow2020@gmail.com**. On March 26, 2025, Google Inc. responded with the following information:

Google Subscriber Information

Google Account ID: 762897971482

Name: Shawn Marlow

Given Name: Shawn

Family Name: Marlow

E-Mail: **shawn.marlow2020@gmail.com**

Created on: 2018-08-28 21:32:13 Z

Account Recovery

Recovery SMS: +14059683540 [US] = T-Mobile

Postal Address

Created on: 2018-11-20 21:35:34 UTC

Postal Code: 73106

Locality Name: Oklahoma City

Address Line: 1729 Northwest 3rd Street

Recipient Name: Shawn Marlow

Phone Number Saved to Address: + 1 405-446-6174

Postal Address

Created on: 2019-11-10 14:07:59 UTC

Postal Code: 73045

Locality Name: Harrah

Postal Code

Address Line: 9633 North Harrah Road

Recipient Name: Shawn Marlow

13. Based on open-source records, it was determined IP addresses 70.182.71.46 and 70.182.93.83 were controlled by Cox Communications. On or about May 6, 2025, an administrative subpoena was served to Cox Communications to provide information pertaining to Kik Login IP addresses: 70.182.93.83 on 2024-10-13 16:58:45 UTC Port 52886

and 70.182.71.46 on 2024-11-10 18:00:02 UTC Port 59740, and 2025-02-16 18:01:00 UTC Port 53556. On or about May 12, 2025, Cox Communications responded with the following regarding both IP addresses:

Name: Nowakoski LLC DBA Tubs of Sud

Address: 3400 S Harrah Rd Harrah, OK 73045-6078

Telephone number: 405-637-5331

14. On April 9, 2025, an administrative subpoena was served to T-Mobile USA, provide information pertaining to telephone number: 405-968-3540. On or about April 22, 2025, T-Mobile USA, Inc. responded with the following information:

Subscriber Name: Ashley Livengood

Subscriber Address: 12629 NE 39th St., Spencer, OK 73084

Subscriber Status: Active

Activation Date: 08/15/2022

15. Open-source checks for Shawn Marlow show an address of 8555 N Dobbs Rd., Harrah, Oklahoma. One of two phone numbers listed for Shawn Marlow from January 2020 to January 2025, is 405-968-3540, the same number associated with the Google email described in paragraph 11. The other listed phone number is 405-827-0865. In addition, a financial record revealed Shawn Marlow with a financial transaction on January 17, 2025. This record listed his associated phone number as 405-968-3540, and his associated address as 8555 N Dobbs Rd, Harrah, OK 73045-8873.

16. The Oklahoma Sex Offender Registry lists Shawn Michael Marlow, date of birth [XX-XX-] 1992, as a registered sex offender as of August 7, 2017, with a completion of

sentence of March 2, 2026. Marlow's listed alias is Shawn Michael Heuer. There are two crimes listed from Osage County, Soliciting Sexual Conduct of Communication with Minor by use of Technology and Asst Lewd Exhibition, both of which have conviction dates of March 3, 2017. The home address for Shawn Marlow on the Oklahoma Sex Offender Registry is 8555 N Dobbs Rd, Harrah, Oklahoma 73045. The Employers listed is TAKE TEN TIRE at 1330 S. Eastern, Oklahoma City, Oklahoma. Shawn Marlow's vehicle listed on the Oklahoma Sex Offender Registry is a dark blue Dodge Ram 1500 (Pickup) with Oklahoma license plate QBW431. On February 14, 2025, the Oklahoma Department of Corrections has a record of Shawn Marlow's Sex Offender Registration and Notice of Duty to Register, with Marlow's address of 8555 N Dobbs Rd., Harrah, Oklahoma 73045, and a primary phone number of 405-827-0865.

EXECUTION OF WARRANTS

17. On or about June 16, 2025, a search warrant was served to Kik for both usernames, smh2022_c3t and smh2022, and on June 17, 2025, a search warrant was served to Google for email address **shawn.marlow2020@gmail.com**. During the review of the Kik returns, law enforcement observed the CSAM video and image Kik submitted to NCMEC, along with associated Kik chats. During the review of the Google return, law enforcement observed multiple emails from Dropbox to MARLOW stating his Dropbox was at its capacity¹. On June 18, 2025, a search warrant was executed on Marlow's person and a search warrant was executed on his vehicle, the 2018 Dodge Ram 1500 with Oklahoma license plate

¹ Google emails reveal Dropbox emailing MARLOW from June 2019 to May 2025. Beginning in August of 2019, Dropbox emails began communicating the Dropbox account was out of space.

QBW431, at Take Ten Tire, 1330 S. Eastern, Oklahoma City, Oklahoma. A Samsung Galaxy S24 cell phone was seized on Marlow's person. During a live preview of the cell phone, the Kik application was observed. The Kik account information on the cell phone revealed a username: smhe2, email: smhe202@yahoo.com, and name: smhe2. The cell phone device phone number was 405-642-8743, and the Google Mail application contained an email address of smhe202@gmail.com. One of the SMS text messages observed between Marlow and an unknown individual on August 5, 2024, contained the following:

Marlow texts, "I've always wanted to have a mother and daughter together lol ... Yea would be so hot ... Would you ever have a 3 way with your daughter". The other individual texts, "Noooooooo".

Marlow was arrested by law enforcement on June 18, 2025, and is currently detained.

18. On June 12, 2025, an administrative subpoena was served to Dropbox for subscriber information associated with **shawn.marlow2020@gmail.com**. On June 17, 2025, Dropbox returned with the following:

User ID: 2261965568

Full Name: Shawn Marlow

Email Address: **shawn.marlow2020@gmail.com**

Account Creation Date: 2019-06-05 13:12:40 UTC

Account Status: Active

Subscription Type: Free

19. A preservation request was submitted to Dropbox on June 30, 2025, to ensure evidence within the Dropbox account associated with **shawn.marlow2020@gmail.com** is

not destroyed.

OVERVIEW OF DROPBOX

20. Dropbox is a personal cloud storage service (sometimes referred to as an online backup service) that is frequently used for file sharing and collaboration, which allows users to share files, to include digital images, movies, and folders with others across the Internet. Dropbox advertises itself as, “a free service that lets you bring your photos, docs, and videos anywhere and share them easily” (www.dropbox.com).

21. The Dropbox application is available for Windows, Macintosh, and Linux desktop operating systems. There are also apps for iPhone, iPad, Android, and BlackBerry devices.

22. Dropbox offers two built-in features to share data with other accounts or individuals. With one feature, a user can move files from one Dropbox account to another using the Shared Folder Option. This method requires a user logging into their Dropbox account via its app or web browser. They then select the files they wish to share and then click on a “Share” tab on the page. A pop-up window will emerge and ask the user to enter the Dropbox email address of the other account with whom they want to share the folder and then will click the “Share” tab on the pop-up window to finish the process. The user of the other Dropbox account will then open their account and click on a “Shared” button which will show the files that have been shared with the user. The user will then click on “Add” to confirm the sharing process and will be able to access the files at any time. The other share feature allows a user to transfer data from one Dropbox account to another via the Shared Link Feature. To do this, a user will open any file or folder from their Dropbox profile that

they intend to share with another account. The user will then click on the “Share” button and then select the “Share with Dropbox” option. A pop-up window will appear, and the user will then click on the “Create Link” button and then copy the link. Anyone with the newly created link will then be able to access the Dropbox files. These sharing features would permit a Dropbox user to share child pornography files between multiple accounts.

23. Dropbox provides a variety of on-line services, including online storage access, to the general public. Dropbox allows subscribers to obtain accounts at the domain name www.dropbox.com. Subscribers obtain a Dropbox account by registering with an email address. During the registration process, Dropbox asks subscribers to provide basic personal identifying information. This information can include the subscriber’s full physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

24. When the subscriber transfers a file to a Dropbox account, it is initiated at the user’s computer, transferred via the Internet to the Dropbox servers, and then can automatically be synchronized and transmitted to other computers or electronic devices that have been registered with that Dropbox account. This includes online storage in Dropbox servers. If the subscriber does not delete the content, the files can remain on Dropbox servers indefinitely. Even if the subscriber deletes their account, it may continue to be available on the Dropbox servers for a certain period of time.

25. Online storage providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session)

times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online storage providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

26. In some cases, Dropbox account users will communicate directly with Dropbox about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Online storage providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

27. This application seeks a warrant to search all responsive records and information under the control of Dropbox, a provider subject to the jurisdiction of this court, regardless of where Dropbox has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Dropbox’s possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

28. As explained herein, information stored in connection with a personal cloud

storage service account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a personal cloud storage service account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, stored communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the provider can show how and when the account was accessed or used. For example, as described below, electronic service providers typically log the Internet Protocol (IP) addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the account owner’s state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Dropbox, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

30. On June 18, 2025, a criminal complaint and arrest warrant were filed in the United States District Court for the Western District of Oklahoma, Case No. M-25-401-STE charging Shawn Michael Marlow with possession of child pornography, a violation of 18 U.S.C. § 2252A(a)(5)(B), and distribution of child pornography, in violation of 18 U.S.C. § 2252A(a)(2). On the same day, Shawn Michael Marlow was arrested and had his initial appearance where he was detained after waiving his detention hearing and preliminary hearing.

31. In sum, MARLOW has been the subject of two different NCMEC tips from Kik, one of which provided his email address **shawn.marlow2020@gmail.com**. During the investigation, law enforcement determined MARLOW used the same email address for a Dropbox account, which he established in 2019, and the account was still showing active as of June 17, 2025. Based on my training and experience individuals who distribute CSAM, also store CSAM in multiple locations, and often in web-based, cloud, storage accounts to

access anytime. Additionally, Dropbox provides users with multiple avenues for sharing files between Dropbox accounts. Based on the foregoing, I believe evidence of violations of 18 U.S.C. § 2252A(a)(5)(B) would be found in the Dropbox account associated with **shawn.marlow2020@gmail.com**, and I request that the Court issue the proposed search warrant.

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

33. The government will execute this warrant by serving the warrant on Dropbox, Inc. Because the warrant will be served on Dropbox, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Marisol Flores
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to before me this 3rd day of July, 2025.



CHRIS M. STEPHENS
United States Magistrate Judge
Western District of Oklahoma

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Dropbox account associated with **shawn.marlow2020@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc. (“Dropbox”), an electronic service provider that accepts service of legal process at 1800 Owens St., Ste. 200 San Francisco, CA 94158.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit card or bank account numbers);
- b. The types of service utilized by the user;
- c. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

d. All records pertaining to communications between the Provider, and any person regarding the account, including contacts with support services and records of actions taken.

e. All user content created, uploaded, or shared by the account;

f. All content data, including but not limited to all file activity logs (i.e., data related to the upload, download, and access of each file); and

g. All images and videos in the account.

The Provider is hereby ordered to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely, possession of child pornography, a violation of Title 18, United States Code, Section 2252A(a)(5)B); the violation involving user or users of the account or identifier listed in Attachment A, including information pertaining to the following matters:

a. the production, distribution, receipt or possession of images of child pornography; or correspondence in furtherance of the commission of offenses involving the production, distribution, receipt or possession of child pornography.

b. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

c. All images depicting children engaging in sexually explicit conduct as

defined in 18 U.S.C. § 2256.